시나리오 제목

입시 전쟁의 보이지 않는 손

– 나이스(Nice) 하지 않은 나이스(NEIS : National Education Information System) 체계 –

시나리오 단계

1단계 : 정찰 및 침투 단계

교사·교육청 직원 계정 탈취를 위한 대상자 탐색 및 피싱 메일을 통해 악성코드 실행 및 내부 네트워크 접속, 직원 계정에서 관리자 권한 탈취

2단계 : 내부망 이동

내부망 접근 및 시스템 탐색을 통한 구조화

3단계 : 정보조작, 탈취

성적, 생활기록부 관리 서버 접근, 데이터 조작 및 로그 삭제, 백도어 설치

4단계 : 사이버 방어

사이버 방어 조치(다중인증, 이상행위 탐지 등)

시나리오 목적

입시 전산망 해킹이라는 가상 상황을 통해 **해킹 공격 절차 이해** 뿐만 아니라 **사이버 위협에 대응**하는 **기술적·사고적 역량을 발전**시키고, **사회적 파급효과와 국가적 차원의 보안 필요성**을 종합적으로 사고하는 데 목적이 있다.

* 해킹 대상 : 나이스 국가교육정보시스템(NEIS : National Education Information System)

① **공격측면** : 피싱, 계정탈취, 내부망 이동, 데이터 조작 등 현실적 위협 시나리오 활용, 모의훈련 실시

② **방어측면** : 탐지–분석–대응–복구 전 과정을 통해 나이스 체계 정보보호 인프라의 취약점을 확인

③ **교육 효과** : 단순 해킹 재현이 아닌, 차세대 보안 기술·운영 훈련을 간접 경험

시나리오 줄거리

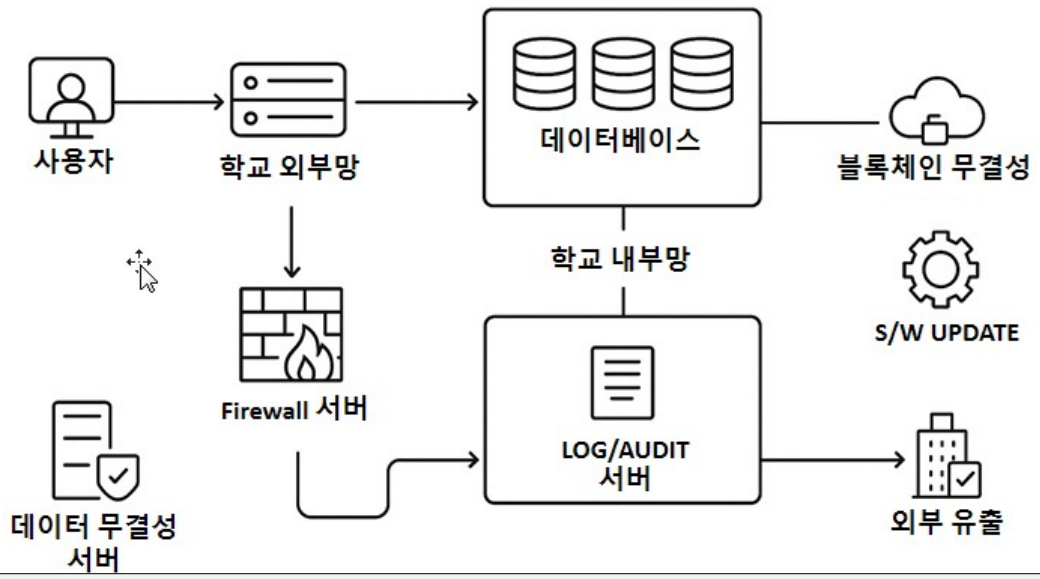
- (배경) 대한민국의 모든 고등학생은 대학입시를 위해 '전쟁'이라 불릴 만큼 치열한 경쟁을 치르고 있다. 학생들의 대학 진학에 있어 가장 중요한 요소는 교육청 전산망에 의해 관리되는 생활기록부와 성적이다. 이 데이터를 조작하면 학생의 운명이 달라질 것이며, 나아가 사회 공정성이 무너지는 심각한 문제를 초래하게 될 것이다.
- (위협등장) 1학기 기말고사가 끝난 시점. 각 학교에서는 생활기록부와 성적을 입력하느라, 교육청 전산 담당자는 체계 오류 등을 해결하느라 정신없는 시기에 교육청 한 전산 담당자가 **피싱 메일**을 받는다. 무심코 클릭한 순간, 해커는 계정 정보를 확보하고, 이를 발판으로 시스템 내부에 침투하여 **권한을 상승** 시킨다.

• (공격시작) 해커는 특정 학생의 생활기록부와 성적 데이터를 은밀히 수정한다. (성적 점수 향상, 수상기록 추가 등) 데이터를 성공적으로 수정한 해커는 **로그를 삭제**하고, **백도어를 설치**해 추적을 회피한다. 동시에, 일부 데이터는 의도적으로 누락시켜 혼란을 증폭시킨다.

• (피해발생) 조작된 데이터로 해당 학생은 인서울 대학 진학에 성공하였지만, 이후 **데이터 무결성 검증 과정**에서 오류가 발견된다. 언론은 이를 **'입시 해킹'**으로 보도하고, 사회는 공정성 붕괴 논란에 빠지게 된다.

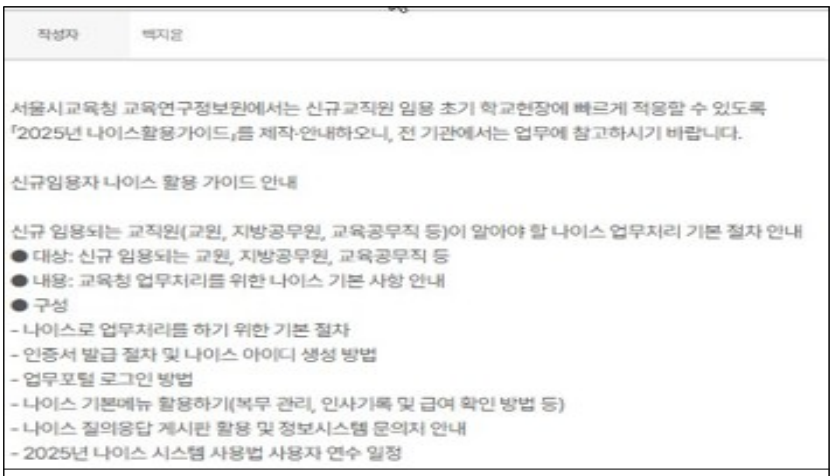
• (대응 및 교훈) 보안 전문가들이 해킹 흔적을 추적하여 피싱 → 권한상승 → 데이터 조작 → 은폐라는 **공격 흐름**을 밝힌다. 이에 따라 다중인증 도입, 이상행위 탐지 시스템 설치, 블록체인 기반 무결성 관리 체계 구축 등 대응방안이 시행된다. 이는 단순 교육 문제 뿐만 아니라 사회적·국가적 보안 문제로 인식하게 된다.

시나리오 네트워크 구성도



Attacker Activity Flow Chart

피싱메일 발송 → 크리덴셜 탈취 → 시스템 로그인 → 네트워크 스캔 → 정보수집 및 목록화 → 권한 상승

<table>
<tr><td colspan="2">단계 번호</td><td>1단계</td></tr>
<tr><td colspan="2">단계 명</td><td>정찰 및 침투</td></tr>
<tr><td colspan="2">주요 목표</td><td>① 교육부 나이스체계 관리담당자 피싱을 위한 메일 설계 및 발송
② 사용자 계정정보 획득, 나이스 체계 데이터 조작을 위한 초기 권한상승 달성</td></tr>
<tr><td rowspan="2">유형</td><td>공격</td><td>취약점 악용, 설치</td></tr>
<tr><td>방어</td><td>-</td></tr>
<tr><td colspan="2">주요 활동</td><td>
① 공격대상 식별
▶ 나이스 체계는 전국 시도교육청 별로 운영되고 있음을 고려하여 해당 지역 교육청의 체계 관리자, 주요 사용자 정보사항 파악
▶ 교육청 홈페이지, 보도자료, 직원 안내문 등을 활용하여 실존 인물과 직위 확인
예) 서울시 교육청 홈페이지 내 체계 운영 관련 담당자 확인

작성자 백지은
서울시교육청 교육연구정보원에서는 신규교직원 임용 초기 학교현장에 빠르게 적응할 수 있도록 「2025년 나이스활용가이드」를 제작·안내하오니, 전 기관에서는 업무에 참고하시기 바랍니다.
신규임용자 나이스 활용 가이드 안내
신규 임용되는 교직원(교원, 지방공무원, 교육공무직 등)이 알아야 할 나이스 업무처리 기본 절차 안내
● 대상: 신규 임용되는 교원, 지방공무원, 교육공무직 등
● 내용: 교육청 업무처리를 위한 나이스 기본 사항 안내
● 구성
- 나이스로 업무처리를 하기 위한 기본 절차
- 인증서 발급 절차 및 나이스 아이디 생성 방법
- 업무포털 로그인 방법
- 나이스 기본메뉴 활용하기(복무 관리, 인사기록 및 급여 확인 방법 등)
- 나이스 질의응답 게시판 활용 및 정보시스템 문의처 안내
- 2025년 나이스 시스템 사용법 사용자 연수 일정
서울시 교육청 홈페이지
* 게시글 작성자를 공격 대상으로 선정

② 피싱 메일 시나리오 작성(예시)
▶ ‘보안 업데이트 안내’, ‘비밀번호 재설정’ 등 긴급하고 설득력 있는 내용 또는 ‘성과상여금’, ‘경조사에 대한 감사 답글’ 등의 흥미를 유발할 수 있는 내용으로 구성
▶ 실제 기관에서 사용하는 화면과 동일하게 로고, 서식 등을 활용하여 신뢰성 강화
</td></tr>
</table>

< 피싱 메일 시나리오 >
보내는 사람 : NEIS관리자(admin@sen.go.kr)
받는 사람 : 000(교육청 실무 담당자)
제 목 : 나이스체계 보안 업데이트 설정 안내

(세부내용 다음 페이지)
안녕하세요.
서울시교육청 교육정보시스템(NEIS) 보안 관리팀입니다.
최근 외부 보안 위협이 증가함에 따라, 시스템 안정성을 강화하기 위해 전체 교직원 계정을 대상으로 긴급 보안 업데이트를 시행합니다.
아래 보안 업데이트 링크를 통해 로그인 후,
사용자 계정 인증 및 보안 패치 적용을 완료해 주시기 바랍니다.
업데이트 미실시 시, 시스템 접근에 제한이 있을 수 있습니다.

[보안 업데이트 바로가기]

감사합니다.
서울시교육청 교육정보시스템(NEIS) 보안 관리팀

③ 메일 발송 준비 및 위장

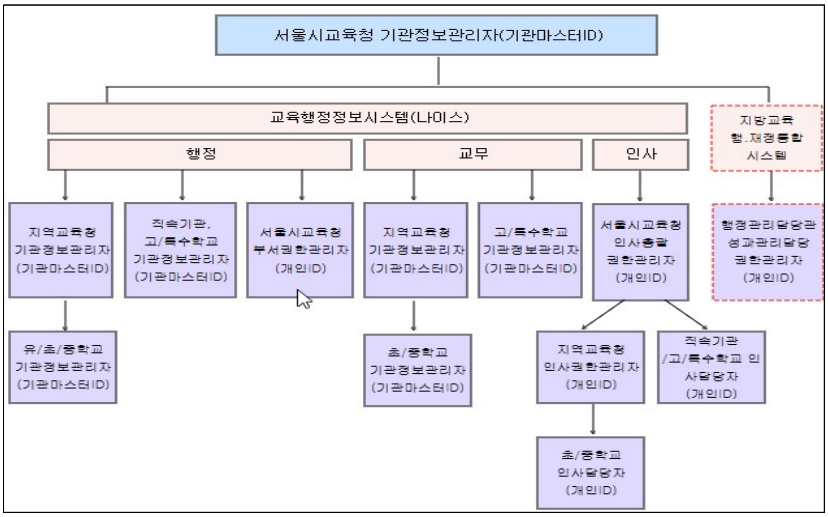
▶ 발신자 주소를 관리자 계정처럼 보이도록 설정
(예. admin@sen.go.kr)

▶ 훈련용 가짜 로그인 페이지 제작(실제 로그인 화면과 유사)

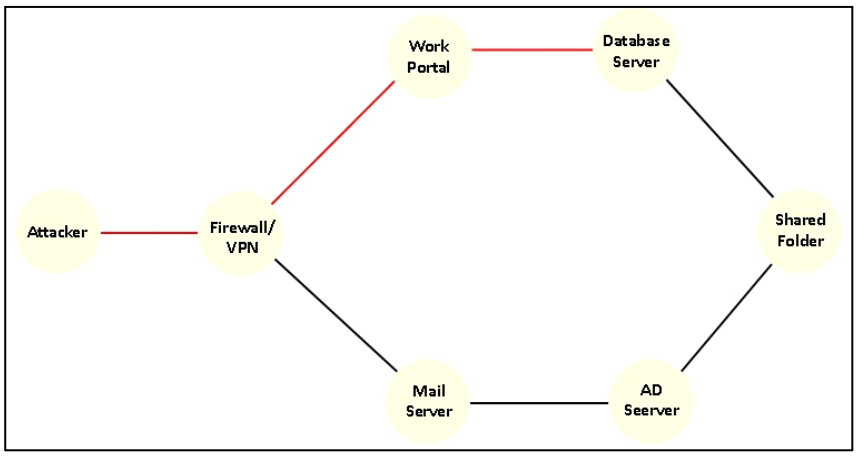
④ 사용자 계정 등 정보 수집

▶ 메일 수신자가 링크 클릭 → 가짜 페이지 접속 → 계정정보(ID / PW) 입력

▶ 입력한 계정정보 공격자 서버로 전송 → 계정정보 확보

	⑤ 초기 권한 상승 ▶ 탈취한 사용자 또는 관리자 계정을 통해 나이스 시스템에 로그인 시도 ▶ 일반 사용자 권한이 아닌 관리자 권한으로 접근 성공 시, 내부망 침투 발판 마련 * 나이스 시스템 관리자 권한 관리 체계(교육청 홈페이지)  ▶ 확보된 계정 정보를 이용하여 추가 시스템 접근(메일 서버, 파일 서버 등) 가능성 확인
주요 사용 도구 및 기술	• **AI 기반 피싱 메일 생성** • **피싱 훈련용 메일 발송 플랫폼** • **HTML 기반 가짜 로그인 페이지 제작 도구** • **계정 크리덴셜(Credential) 수집 및 저장 스크립트** • **관리자/사용자의 심적 동요를 일으킬 수 있는 사회적 기법 (긴급성 강조, 신뢰성 확보, 관리자의 권위 강조 등)**
예상 결과물 및 상태	• **예상 결과물** ▶ 관리자/사용자 피싱을 위한 창의적인 내용이 포함된 메일 완성본 ▶ 사용자가 [보안 업데이트 바로가기] 클릭 시 나타나는 가짜 로그인 페이지 • **예상 상태** ▶ 관리자 권한 확보로 나이스 체계 내 정보조작, 정보유출이 가능한 상태

<table>
<tr><td colspan="2">단계 번호</td><td>2단계</td></tr>
<tr><td colspan="2">단계 명</td><td>내부망 이동</td></tr>
<tr><td colspan="2">주요 목표</td><td>① 탈취한 계정을 이용해 나이스 내부망에 직접 접속하고, 실제 업무 시스템 접근 가능 여부 확인
② 내부망 서버, 데이터베이스, 네트워크 구조 파악으로 공격 확산 기반 마련
③ 내부망 내 권한 상승 및 확대 가능성 검증</td></tr>
<tr><td rowspan="2">유형</td><td>공격</td><td>정찰, 취약점 악용</td></tr>
<tr><td>방어</td><td>-</td></tr>
<tr><td colspan="2">주요 활동</td><td>① 내부망 로그인 및 접근 확인
▶ 1단계에서 확보한 관리자 계정으로 나이스 시스템 접속
▶ 네트워크 방화벽, VPN, IDS 등 보안 장치 우회 여부 확인
▶ 내부 시스템 접근 가능 범위(업무 포털, DB 서버, 메일 서버 등) 탐색

② 시스템 및 네트워크 구조 파악
▶ 내부 IP 대역 스캔을 통해 서버, 단말, 네트워크 장비 식별
▶ DNS, AD(Active Directory) 등 인증 인프라 위치 확인
▶ 공유 폴더, 문서 관리 시스템 등 접근 가능한 저장소 확인
 

< 네트워크 다이어그램 - 인터넷 접근 구조도(예) >

③ 정보수집
▶ 서버 OS 종류, 버전, 패치 현황 확인
▶ 관리자/사용자 계정 목록 및 권한 레벨 수집
▶ 로그 분석을 통해 접근 패턴 및 보안 모니터링 여부 확인</td></tr>
</table>

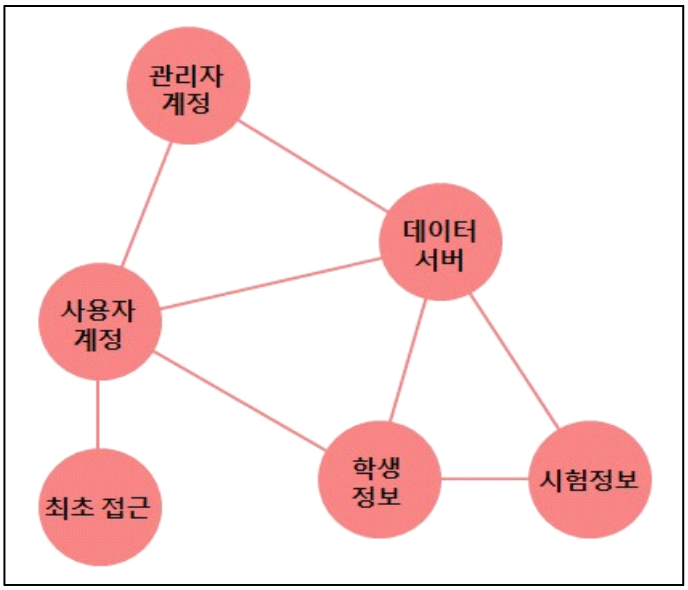
<table>
<tr><td></td><td>

④ 권한 확대 준비

▶ 확보한 계정이 특정 서비스(메일, 전자결재 등)에만 제한될 경우, 추가적인 계정 탈취 시도

▶ 내부망에서 다른 서버로 이동할 수 있는 경로 확보 (시험지 유출 등)

▶ 네트워크 구간별 접근 권한(서버실, DB망, 업무망 등) 구분 확인



< 권한 확대에 따른 데이터 접근 구조도 >

⑤ 은폐 및 지속성 확보

▶ 초기 탐지되지 않도록 로그 조작 또는 흔적 조작

▶ 훈련용 악성 스크립트 삽입 → 실제상황 모사

▶ 일정 시간 간격으로 내부망 연결 유지 여부 점검

</td></tr>
<tr><td>주요 사용 도구 및 기술</td><td>

• 내부망포트 스캐너(Advanced Port Scanner, Nmap 등)

• 자격증명 덤핑(Credential Dumping) 도구(훈련용 시뮬레이터)

• 네트워크 트래픽 분석 도구(Wireshark, SolarWinds 등)

• Active Directory 및 계정 탐색 툴(PowerShell 등)

• 로그 분석 및 위조 도구

</td></tr>
<tr><td>예상 결과물 및 상태</td><td>

• 예상 결과물

▶ 내부망 구조도(서버, 네트워크, 계정 관계) 확보

▶ 주요 계정 권한 관계, 접근 가능한 서비스 리스트

▶ 추가 시스템 접근 경로와 공격 확산 가능성 확인

• 예상 상태

▶ 권한상승 및 권한확대 기반 조성

▶ 보안 관제에서 얼마나 탐지되는지 여부 확인 가능

</td></tr>
</table>

<table>
<tr><td colspan="2">단계 번호</td><td>3단계</td></tr>
<tr><td colspan="2">단계 명</td><td>정보조작, 탈취</td></tr>
<tr><td colspan="2">주요 목표</td><td>① 공격자는 확보한 권한을 활용하여 중요 데이터(운영 정보, DB 기록, 성적·출결 등)를 조작하거나 훼손, 정보 신뢰성 저하
② 로그 삭제 및 위조를 통해 남긴 흔적 제거, 정상 사용자 행위로 위장하여 활동을 은폐
③ 보안솔루션을 무력화, 우회하여 탐지를 회피하고, 지속적으로 내부망에 은폐된 상태로 장악상태 유지</td></tr>
<tr><td rowspan="2">유형</td><td>공격</td><td>설치, 명령 및 제어, 목표 달성</td></tr>
<tr><td>방어</td><td>-</td></tr>
<tr><td colspan="2">주요 활동</td><td>① 데이터 조작
▶ DB 내 특정 값 변경(예 : 로그인 기록, 사용자 계정 권한)
▶ 중요 문서나 생활기록부 일부 훼손 또는 은밀한 수정 (예 : 학교성적, 상훈, 학생회 활동 등)
▶ 수천 건 데이터 동시 변조 / 노이즈 삽입 공격(시스템 혼란 유발)
▶ 입시에 반영되는 자료 변조로 입시체계 혼란 유발
 

< 실제 나이스 체계 내 입력내용 >

② 로그 삭제 및 위조
▶ 윈도우 이벤트 로그, DB 접속 로그 제거
▶ 정상 사용자 활동처럼 위장하여 탐지 회피
▶ 보안관제 로그와 백업본 불일치를 발생시켜 추적 지연</td></tr>
</table>

	③ 방어 조치 무력화 ▶ 백신/EDR 서비스 종료 시도, 프로세스 강제 중단 ▶ Rootkit 및 탐지 규칙 우회 기법 적용 ▶ 지속적 접근을 위한 백도어 설치 및 은닉
주요 사용 도구 및 기술	• **데이터 변조, 윈도우 로그 삭제(Revo Uninstaller) 등 프로그램** • **이벤트 로그 명령 기반 삭제, 보안 솔류션 프로세스 종료** • **Rootkit 기반 은폐 기법, 백도어 생성기**
예상 결과물 및 상태	• 핵심 데이터 조작으로 **입시체계 및 행정 업무 혼란** 발생 • 로그 흔적 제거 및 위장으로 **장기간 활동 은폐** • **내부망에 지속적 접근** 통로 확보

<table>
<tr><td colspan="2">단계 번호</td><td>4단계</td></tr>
<tr><td colspan="2">단계 명</td><td>사이버 방어</td></tr>
<tr><td colspan="2">주요 목표</td><td>① 공격자가 수행한 데이터 변조·로그 삭제·백도어 설치 행위를 탐지하고 차단
② 무결성 검증 체계를 통해 위·변조된 데이터를 식별 및 복구
③ 다층 보안 구조(이상행위 탐지, 로그 중앙화, 네트워크 분리 등)를 통해 향후 재발 방지 체계를 구축
④ 기술적·제도적 조치를 결합하여 지속 가능한 방어 인프라를 완성</td></tr>
<tr><td rowspan="2">유형</td><td>공격</td><td>-</td></tr>
<tr><td>방어</td><td>탐지, 분석, 대응</td></tr>
<tr><td colspan="2">주요 활동</td><td>방어자 측면
① 탐지단계
▶ IDS/IPS, 이상행위 탐지시스템에서 비정상 행위 감지
▶ 관리자 계정 다중 로그인 시도, 비인가 접속 알림 확인

② 분석단계
▶ 로그 백업과 현재 로그 비교로 삭제·위조 여부 확인
▶ DB 무결성 검증 툴을 이용해 데이터 변조 여부 판별
▶ 보안 이벤트를 SOC에서 상관 분석

③ 대응/복구단계
▶ 의심계정 차단, 세션 강제 종료
▶ 백도어 탐색 및 제거
▶ DR(Disaster Recovery) 센터를 통한 정상 데이터 복구

④ 사후 강화 단계
▶ 다중인증(MFA) 도입 및 전사 계정 정책 강화
▶ 블록체인 기반 무결성 관리 체계 도입 검토
▶ WORM(Write Once Read Many) 스토리지, DB 이중화 무결성 체크
▶ 피싱 대응 모의 훈련 및 보안의식 제고
▶ 구간망 분리, USB 차단 등 제도적 통제 보완</td></tr>
</table>

주요 사용 도구 및 기술	• IDS/IPS, EDR, 사용자 및 엔터티 동작분석(UEBA) 기반 이상행위 탐지 시스템 • DB 무결성 검증 툴, 로그 관리/분석 시스템 (보안 정보 및 이벤트 관리, SIEM) • 중앙화된 SOC(Security Operation Center) 솔루션 • DR센터 복구 솔루션 • 다중인증(MFA) 시스템, 블록체인 무결성 관리 솔루션
예상 결과물 및 상태	• 방어자 측면 ▶ 위·변조된 데이터 탐지 및 복구 성공 ▶ 로그 조작 행위 확인 및 증거 확보 ▶ 백도어 제거 및 정상 서비스 복원 ▶ 탐지-분석-대응-사후강화로 이어지는 보안 사이클 완성 • 공격자 측면 ▶ 은폐 무력화, 장기 침투 실패 ▶ 재진입 시도 시 강화된 보안 체계에 의해 차단